What is claimed is:

1   1. A cryptocommunication system including a

2 transmission apparatus and a reception apparatus,

3   the transmission apparatus encrypting plaintext to

4 generate ciphertext, performing a one-way operation on the

5 plaintext to generate a first value, and transmitting the

6 ciphertext and the first value to the reception apparatus,

7   the reception apparatus receiving the ciphertext and

8 the first value, decrypting the ciphertext to generate

9 decrypted text, performing the one-way operation on the

10 decrypted text to generate a second value, and judging that

11 the decrypted text matches the plaintext when the second value

12 and the first value match,

13   the transmission apparatus comprising:

14   first generating means for generating first additional

15 information;

16   first operation means for performing an invertible

17 operation on the plaintext and the first additional

18 information to generate connected information;

19   encrypting means for encrypting the connected

20 information according to an encryption algorithm to generate

21 the ciphertext; and

22   transmitting means for transmitting the ciphertext,

23   the reception apparatus comprising:

24   receiving means for receiving the ciphertext;

25   second generating means for generating second

26   additional information which is identical to the first

27   additional information;

28   decrypting means for decrypting the ciphertext

29   according to a decryption algorithm which is an

30   inverse-conversion of the encryption algorithm so as to

31   generate decrypted connected information; and

32   second operation means for performing an inverse

33   operation of the invertible operation on the decrypted

34   connected information and the second additional information

35   so as to generate the decrypted text.

1   2.   The cryptocommunication system of Claim 1,

2   wherein the second generating means synchronizes with

3   the first generation means so as to generate the second

4   additional information which is identical to the first

5   additional information.

1   3.   The cryptocommunication system of Claim 1,

2   wherein the first generating means transmits the first

3   additional information, and

4   the second generating means receives the first

5   additional information and sets the received first additional

6   information as the second additional information.

1   4.   The cryptocommunication system of Claim 1,

2   wherein the first generating means encrypts the first

3   additional information according to the encryption algorithm

4   to generate encrypted additional information, and transmits

5   the generated encrypted additional information, and

6   the second generating means receives the encrypted

7   additional information, and decrypts the received encrypted

8   additional information according to the decryption algorithm

9   which is an inverse-conversion of the encryption algorithm

10   to generate additional information, and sets the generated

11   additional information as the second additional information.

1   5.   The cryptocommunication system of Claim 1,

2   wherein the first generating means generates a random

3   number, and sets the generated random number as the first

4   additional information.

1   6.   The cryptocommunication system of Claim 1,

2   wherein the invertible operation means bit-connects

3   the plaintext with the first additional information so as

4   to generate the connected information, and

5   the second operation means deletes the second

6   additional information from the decrypted connected

7   information to generate the decrypted text.

1   7.   The cryptocommunication system of Claim 1,

2   wherein the first operation means performs an

3   exclusive OR operation on the plaintext and the first

4   additional information to generate the connected information,

5   and

6   the second operation means performs an exclusive OR

7   operation on the decrypted connected information and the

8   second additional information to generate the decrypted text.

1   8.   The cryptocommunication system of Claim 1,

2   wherein the first operation means adds the first

3   additional information to the plaintext to generate connected

4   information, and

5   the second operation means subtracts the second

6   additional information from the decrypted connected

7   information to generate the decrypted text.

1   9.   The cryptocommunication system of Claim 1,

2   wherein the first operation means performs modular

3   multiplication on the plaintext and the first additional

4   information to generate the connected information, and

5   the second operation means performs modular

6   multiplication on the decrypted connected information and

7   the modular inversion of the second additional information

8   to generate the decrypted text.

1   10.   The cryptocommunication system of Claim 1,

2   wherein the first operation means replaces the

3   plaintext expressed in bit based on the first additional

4   information to generate the connected information,

5   and the second operation means inverse-replaces the

6   decrypted connected information expressed in bit based on

7   the second additional information to generate the decrypted

8   text.

1   11.   The cryptocommunication system of Claim 1,

2   wherein the first operation means stores, in advance,

3   a conversion table corresponding to the first additional

4   information, and converts the plaintext according to the

5   conversion table to generate the connected information, and

6   the second operation means stores, in advance, a

7   conversion table corresponding to the second additional

8   information and being identical to the conversion table

9   corresponding to the first additional information, and

10   converts the decrypted connected information in a reverse

11   direction according to the conversion table to generate the

12   decrypted text.

1   12.   The cryptocommunication system of Claim 1,

2   wherein when the transmission-apparatus-encrypts, in

3   order to generate ciphertext, the plaintext that has been

4   encrypted and transmitted, and transmits the newly generated

5   ciphertext to the reception apparatus,

6   and the reception apparatus receives the newly generated

7   ciphertext and decrypts the newly generated ciphertext,

8   the first generating means generates third additional

9   information which is different from the first additional

10   information,

11   the first operation means performs an invertible

12   operation on the plaintext and the third additional

13   information to obtain newly generated connected information,

14   the encrypting means encrypts the newly generated

15   connected information according to an encryption algorithm

16   to obtain the newly generated ciphertext,

17   the transmitting means transmits the newly generated

18   ciphertext,

19   the receiving means receives the newly generated

20   ciphertext,

21   the second generating means generates forth additional

22   information which is identical to the third additional

23   information,

24   the decrypting means decrypts the newly generated

25   ciphertext according to a decryption algorithm which is an

26   inverse-conversion of the encryption algorithm to obtain newly

27   generated decrypted connected information,

28   and the second operation means performs an inverse

51

29 operation of the invertible operation on the newly generated

30 decrypted connected information and the fourth additional

31 information to obtain newly generated decrypted text.

1 13. The cryptocommunication system of Claim 1,

2 wherein the transmission apparatus performs the

3 one-way function on the connected information instead of on

4 the plaintext, in order to generate the first functional value,

5 the reception apparatus performs the one-way function

6 on the decrypted connected information instead of on the

7 decrypted text, in order to generate the second functional

8 value,

9 and the reception apparatus judges whether the first

10 and the second functional values match.

1 14. The cryptocommunication system of Claim 1,

2 wherein the transmission apparatus further performs,

3 on the plaintext, a different invertible operation from the

4 invertible operation, to generate first connected

5 information,

6 the transmission apparatus performs the one-way

7 function on the first connected information, instead of on

8 the plaintext, to generate the first functional value,

9 the reception apparatus further performs the

10 different invertible operation on the decrypted text to

52

11 generate second connected information,

12 the reception apparatus performs the one-way function

13 on the second connected information instead of on the decrypted

14 text, to generate the second functional value,

15 and the reception apparatus judges whether the first

16 and the second functional values match.

1 15. A cryptocommunication method used by a

2 cryptocommunication system including a transmission

3 apparatus and a reception apparatus,

4 the transmission apparatus encrypting plaintext to

5 generate ciphertext, performing a one-way operation on the

6 plaintext to generate a first value, and transmitting the

7 ciphertext and the first value to the reception apparatus,

8 the reception apparatus receiving the ciphertext and

9 the first value, decrypting the ciphertext to generate

10 decrypted text, performing the one-way operation on the

11 decrypted text to generate a second value, and judging that

12 the decrypted text matches the plaintext when the second value

13 and the first value match,

14 the cryptocommunication method including a transmission

15 step which is executed by the transmission apparatus and a

16 reception step which is executed by the reception apparatus,

17 the transmission step comprising:

18 a first generating substep for generating first

19 additional information;

20   a first operation substep for performing an invertible

21 operation on the plaintext and the first additional

22 information to generate connected information;

23   an encrypting substep for encrypting the connected

24 information according to an encryption algorithm to generate

25 the ciphertext; and

26   a transmitting substep for transmitting the ciphertext,

27   the reception step comprising:

28   a receiving substep for receiving the ciphertext;

29   a second generating substep for generating second

30 additional information which is identical to the first

31 additional information;

32   a decrypting substep for decrypting the ciphertext

33 according to a decryption algorithm which is an

34 inverse-conversion of the encryption algorithm so as to

35 generate decrypted connected information; and

36   a second operation substep for performing an inverse

37 operation of the invertible operation on the decrypted

38 connected information and the second additional information

39 so as to generate the decrypted text.

1   16. Cryptocommunication program used by a

2 cryptocommunication system including a transmission

3 apparatus and a reception apparatus,

4   the transmission apparatus encrypting plaintext to

5   generate ciphertext, performing a one-way operation on the

6   plaintext to generate a first value, and transmitting the

7   ciphertext and the first value to the reception apparatus,

8   the reception apparatus receiving the ciphertext and

9   the first value, decrypting the ciphertext to generate

10   decrypted text, performing the one-way operation on the

11   decrypted text to generate a second value, and judging that

12   the decrypted text matches the plaintext when the second value

13   and the first value match,

14   the cryptocommunication program including a

15   transmission step which is executed by the transmission

16   apparatus and a reception step which is executed by the

17   reception apparatus,

18   the transmission step comprising:

19   a first generating substep for generating first

20   additional information;

21   a first operation substep for performing an invertible

22   operation on the plaintext and the first additional

23   information to generate connected information;

24   an encrypting substep for encrypting the connected

25   information according to an encryption algorithm to generate

26   the ciphertext; and

27   a transmitting substep for transmitting the ciphertext,

28   the reception step comprising:

55

29   a receiving substep for receiving the ciphertext;

30   second generating means for generating second

31 additional information which is identical to the first

32 additional information;

33   a decrypting substep for decrypting the ciphertext

34 according to a decryption algorithm which is an

35 inverse-conversion of the encryption algorithm so as to

36 generate decrypted connected information; and

37   a second operation substep for performing an inverse

38 operation of the invertible operation on the decrypted

39 connected information and the second additional information

40 so as to generate the decrypted text.

1   17. A recording medium which can be read from using a

2 computer and which stores cryptocommunication program used

3 by a cryptocommunication system including a transmission

4 apparatus and a reception apparatus,

5   the transmission apparatus encrypting plaintext to

6 generate ciphertext, performing a one-way operation on the

7 plaintext to generate a first value, and transmitting the

8 ciphertext and the first value to the reception apparatus,

9   the reception apparatus receiving the ciphertext and

10 the first value, decrypting the ciphertext to generate

11 decrypted text, performing the one-way operation on the

12 decrypted text to generate a second value, and judging that

13 the decrypted text matches the plaintext when the second value

14 and the first value match,

15   the cryptocommunication program including a

16 transmission step which is executed by the transmission

17 apparatus and a reception step which is executed by the

18 reception apparatus,

19   the transmission step comprising:

20   a first generating substep for generating first

21 additional information;

22   a first operation substep for performing an invertible

23 operation on the plaintext and the first additional

24 information to generate connected information;

25   an encrypting substep for encrypting the connected

26 information according to an encryption algorithm to generate

27 the ciphertext; and

28   a transmitting substep for transmitting the ciphertext,

29   the reception step comprising:

30   a receiving substep for receiving the ciphertext;

31   a second generating substep for generating second

32 additional information which is identical to the first

33 additional information;

34   a decrypting substep for decrypting the ciphertext

35 according to a decryption algorithm which is an

36 inverse-conversion of the encryption algorithm so as to

37 generate decrypted connected information; and

38   a second operation substep for performing an inverse

39   operation of the invertible operation on the decrypted

40   connected information and the second additional information

41   so as to generate the decrypted text.

1   18. A transmission apparatus which encrypts plaintext

2   to generate ciphertext, performs a one-way operation on the

3   plaintext to generate a first value, and transmits the

4   ciphertext and the first value, the transmission apparatus

5   comprising:

6   first generating means for generating first additional

7   information;

8   first operation means for performing an invertible

9   operation on the plaintext and the first additional

10   information to generate connected information;

11   encrypting means for encrypting the connected

12   information according to the encryption algorithm to

13   generate ciphertext; and

14   transmitting means for transmitting the ciphertext.

1   19. A reception apparatus which receives, from a

2   transmission apparatus, ciphertext and a first value, decrypts

3   the ciphertext to generate decrypted text, performs the

4   one-way operation on the decrypted text to generate a second

5   value, and judges that the decrypted text corresponds to the

6   plaintext only when the second value and the first value match,

7   the transmission apparatus encrypting the plaintext to

8   generate the ciphertext, performing the one-way operation

9   on the plaintext to generate the first value, and transmitting

10 the ciphertext and the first value,

11   the reception apparatus comprising:

12   receiving means for receiving the ciphertext from the

13 transmission apparatus of Claim 18;

14   second generating means for generating second

15 additional information which is identical to the first

16 additional information;

17   decrypting means for decrypting the ciphertext

18 according to a decryption algorithm which is an

19 inverse-conversion of the encryption algorithm to generate

20 decrypted connected information; and

21   second operation means for performing an inverse

22 operation of the invertible operation on the decrypted

23 connected information and the second additional information

24 to generate decrypted text.

59